LAW360

Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Forensic Analytics Can Find Needles In Multiple Haystacks

Law360, New York (April 30, 2013, 3:23 PM ET) -- Forensic analytics is indispensable to any situation involving voluminous transactions or other large amounts of data. Forensic analytics enables investigators and litigators to develop smoking gun evidence. It empowers compliance officers and auditors to prevent and detect misconduct even in the absence of an allegation or suspicion. Finance and business personnel can leverage forensic analytics to attack revenue and expenditure leakage and cut by half the 4 percent of earnings that 20 percent of companies lose annually to misconduct.

Forensic analytics provides more coverage, cuts costs and saves time. It permits analysis of an entire data population as opposed to statistical samples. Manual review requires a large team of analysts and voluminous man-hours of work. Forensic analytics uses a programmatic approach that is not only efficient in terms of processing time, but produces exact results fitting the investigative model. It facilitates more frequent and timely assessments, and improves ability to respond to urgent events, reducing both the time it takes to uncover a fraud and its overall impact to the organization.

NOT employing forensic analytics or doing so poorly is perilous in today’s data rich environment. How, for example, do the company and its compliance officer defend the compliance program against a government claim that forensic analytics would have prevented, or more timely detected, corporate misconduct? How does a chief audit executive, controller or business leader rationalize undetected leakage and fraud when subsequent investigation reveals red flags that they could have noticed had they used forensic data analytics? How does a litigator justify to the client a failure to discover critical information that the party opponent discovered through forensic analytics?

Nonetheless, too few organizations use forensic analytics and, with exceptions, rarely maximize its potential. Do they mistakenly think that forensic analytics is too expensive or time consuming? Do they fear computer geeks speaking technobabble?

This article summarizes, in nontechnical terms, the forensic analytics process. The recently publicized European soccer match-fixing scandal provides a handy illustration. By way of background, the soccer match-fixing scandal involves a 19 month global investigation by Europol and Singaporean law enforcement authorities. According to press reports, the investigators have identified 425 professional soccer players and team officials who Europol suspects rigged 680 Europa League matches for an organized crime gambling syndicate. Government investigators remain tight-lipped about the investigation and the specific matches, teams and players currently in their crosshairs.

While we only can speculate about the use of forensic analytics, one thing seems clear: with such a large population of dubious matches and suspected players, a data trail invariably exists to identify other suspicious matches. In preparing this article, for example, StoneTurn compared betting money line statistics with historical data for the Europa League from July 2008 through December 2012. Our quick, high level analysis identified three teams that had a higher than expected percentage of losses when they were heavily favored. These results were not proof of impropriety; rather, they were risk indicators warranting follow up inquiry, which led us to conclude that they are likely false positives.

Forensic analytics is as important for prevention and detection as it is for investigation. The Europa League might have possibly avoided this scandal, if they had invested modestly to develop and run analytic models to deter and timely detect match fixing.

Assemble Multidisciplinary Experts

Projects range from the very simple to the highly complex. Most projects require multidisciplinary experts in forensic risks and controls, computer programming data analysis and investigation. Following is a high level summary of the process.

1. Identify potential scenarios
2. Develop risk indicators and data tests
3. Collect, assimilate and analyze data
4. Investigate and eliminate "false positives"

Identify Potential Scenarios

The resources needed for this step depend on whether the matter involves (1) an investigation of specific allegations (reactive) or (2) prevention and detection in absence of a suspicion or allegation (proactive). In an investigation, the team typically understands the scenario with a fair amount of specificity. For matters involving prevention and detection, the forensic analytics team will need forensic risks and controls experts in identifying inherent vulnerabilities, evaluating design and operating effectiveness of controls, developing fraud and corruption risk indicators.

The soccer match-fixing scandal illustrates forensic analytics as an investigative tool. To maximize forensic analytics, the forensic analytics team needs to gain a very detailed understanding of the intricacies of soccer gambling. Press reports reveal that soccer gambling extended beyond win or lose. One newspaper article, for example, described a rigged match where a Singaporean gambler allegedly promised to pay players 100,000 euros if, in a game involving Italy’s second-tier league, they arranged for their team to (1) avoid allowing any goals in the first 15 minutes of the match, (2) have at least three total goals scored, (3) have at least a two-goal difference in the final score and (4) lost the game.

The practicalities of an investigation require the forensic analytics team to make assumptions about scheme mechanics. There are a myriad of wagering options for any sporting event, and each would require customized analytic tests to search for anomalies. The most general, and easily illustrative, example for soccer is wagering the money-line where a bettor picks a team to win, lose or tie. Each option would contain a favorite (requiring a larger wager to win $100) and an underdog (a smaller bet to win $100.).

Newspaper reports indicate that scheme involved players who were purposefully manipulating the outcome of matches. For a match-fixer to approach a player and say "play extra hard to win this game" leaves too many variables to chance. The more likely scenario is to convince players to ensure a loss: low energy play, blown defensive assignments and high-turnovers allow a fixer to create opportunities for the other team to win.

If organized crime gambling underlies match fixing, the team likely will focus on potential payout. To manipulate the results for a match with a 1:1 money-line payout (or worse) is likely not worth the risk. A bettor would receive a substantially higher payday if they could manipulate a match so that a heavy favorite loses a match. Therefore, specific analytic attention would be paid to current and historical matches were a heavily favored team falls to an inferior opponent per the money-line designations. The team might also assume that organized crime members would use the same players, officials and/or teams to assist in the fixing scheme, as the syndicate presumably has access to only a limited circle of players. The analytic thus might track and search for patterns of movement of players across teams.

If the goals were deterrence and detection in absence of an allegation, the team would need to take a broader view and consider the "who," "what," "where," "when" and how soccer matches might be manipulated. The team, for example, would need to interview team officials, players, referees and others in a position to manipulate and ask "the devil" questions, e.g., what results could you manipulate and how would you go about it? They would also research and catalogue other instances of match-fixing, both in soccer and other sports. The team, for example, would need to study the alleged bribery of a FIFA referee, Edílson Pereira de Carvalho, in Brazil as well as the referee Tim Donaghy NBA basketball scandal.

Develop Risk Indicators and Data Tests

This typically is the most difficult step, particularly in the absence of a specific allegation or suspicion. A traditional investigation typically yields red flags which the organization could or should have spotted to prevent or more timely detect the misconduct. Forensic risks and controls experts refer to these red flags as "risk indicators" because they indicate potential misconduct.

In the absence of a specific allegation or suspicion, the forensic risks and controls expert must devise risk indicators by imagining or the red flags that would arise, if it were conducting an investigation into scenarios identified during step one. Creativity is essential, as is a deep understanding of types and sources of data. Advances in forensic analytics make it possible and practical to compare data from multiple sources, e.g., the organization's current and retired information systems, counterparties, vendors, customers, joint venture partners, and public sector and commercial databases.

Next, the team culls risk indicators that might be detected through data anomalies and outliers. Forensic analytics experts employ a broad spectrum of analyses, including rules based, predictive, linking and social network analysis. The team must be able to develop software code to run these tests.

In our soccer match-fixing illustration, a risk factor might involve, for example, patterns pertaining to heavy favorites who lose or fail to meet other variables such as number of goals scored, difference of total score, etc. The team must be able to design tests that compare data from soccer leagues with online gambling and sports betting casinos. The team must also be able to integrate non-soccer data developed during the investigation, e.g., timing of texts, contents of email messages, travel of suspect players. The forensic analytics team would develop and run a suite of tests, each searching for "red-flag" indicators of suspect conduct.

Collect, Assimilate and Analyze Data

This step is the bread and butter of experts in forensic analytics, who are experienced in collecting and assimilating data and constructing a specialized database.

The first step involves acquiring and loading the data into the analysis environment. Next, the forensic analytics experts assess data quality, completeness and format. The team also considers the need for transforming data. Say, for example, that the data includes geographic information. The forensic analytics expert must be able to train the computer that "16th Street" is the same as "Sixteenth Street" or that "I Street" is the same as "Eye Street." On international engagements, the team must be able to teach the computer to recognize and translate multiple languages. The forensic data analytics might also enrich the data; say adding data elements from third-party reference data. If the project involves a broker-dealer, for example, the team might add reference data regarding issuer or product type.

By way of illustration, in writing this article, we compared historical match results against money lines. Our analysis identified three teams that had a higher than expected percentage of losses when they were heavily favored. The forensic analytics team would develop additional inquires as more data and information becomes available. It might, for example, flag fluctuations in betting activity, i.e., spikes in volume bet for on suspect teams, or individual player statistics. Like peeling an onion, each analysis produces troubling patterns and leads for the counsel and the organization to investigate.

Investigate and Eliminate "False Positives"

Anomalies prove nothing. The fact that an organization or individual is flagged in a particular data test does not, in and of itself, prove any impropriety. Rather, these tests indicate the need for additional, but focused, investigation.

In the context of forensic analytics, “false positive” refers to instances where followup investigation of a data anomaly uncovers no misconduct. For example, we determined that our analysis of heavily favored teams was a false positive. The analysis flagged three teams as having a high percentage of losses in matches where the team was heavily favored to win. It turned out that the three teams flagged were heavy favorites in only a very few matches, which skewed the results when reported in terms of a percentage.

All false positives are not created equal, nor does a false positive mean that the data analytic is useless or a waste of time. On the contrary, the better forensic analytics experts seek to design tests that produce useful results, even if they do not lead to detection of misconduct. Assume, for example, that an organization identifies sales discounts to distributors as a potential corruption risk and uses forensic analytics to compare discounts offered by sales personnel. Assume also that the test flagged a particular employee for extending an inordinate number of discounts, but that investigation revealed no corrupt activity. The false positive nonetheless would be of interest in management in curtailing revenue leakage.

* * *

Forensic analytics applies across nearly every industry and litigation practice. The cost is a pittance compared to potential benefits. Looking for suspicious activity in a bank? Check for high-frequency $9,000 - $9,999 deposits to avoid mandatory SAR filings. Looking for potential layering activity in the stock market? Check for multiple bid and pull transactions leading up to high-volume sales. Looking for accounts payable fraud? Check for ghost vendors to trending payment activity to vendors over time.

Situations involving numerous transactions or massive amounts of data almost always leave a data trail available to be analyzed. And as the soccer world is finding out, fraud can’t hide within these datasets for very long. Whether you are in finance trying to cut waste, a compliance officer seeking to prevent and detect misconduct, a forensic auditor conducting a corruption review, an investigator responding to allegations or litigator trying to win the case, once you start looking, the data will tell what you need to know.

—By Jonny Frank and Alex Lefferts, StoneTurn Group LLP

Jonny Frank, a partner in the New York office of the StoneTurn Group, served as a federal prosecutor for 12 years and as a PwC partner for 14 years, where he founded and led Fraud Risks & Controls. Mr. Frank also taught Fraud Management, Criminal Investigations, and International Criminal Law at the Yale School of Management, Fordham University, and Brooklyn Law School.

Alex Lefferts, a managing director in the Boston office of the StoneTurn Group has more than 10 years’ experience conducting forensic analytics at Deloitte and StoneTurn, including projects involving prevention, detection and investigation of fraud and misconduct and damage quantification.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.